

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

USDC SDNY  
DOCUMENT  
ELECTRONICALLY FILED  
DOC #:  
DATE FILED: MAR 12 2020

KCG Holdings, Inc., *et al.*,

Plaintiffs,

—v—

Rohit Khandekar,

Defendant.

17-CV-3533 (AJN)

OPINION & ORDER

ALISON J. NATHAN, District Judge:

KCG, a financial-services firm, brings this action against a former employee, Rohit Khandekar. KCG alleges that Khandekar improperly acquired and used several of its trade secrets between November 2016 and May 2017. The parties have cross moved for summary judgment.

The Court grants and denies summary judgment in part to each party. KCG is entitled to summary judgment on its breach-of-contract, Defend Trade Secrets Act, and New York common-law claims. KCG is also entitled to summary judgment on Khandekar's breach-of-contract and bad-faith counterclaims. Khandekar is entitled to summary judgment on KCG's claim under the Computer Fraud and Abuse Act. Khandekar is ORDERED to pay KCG's attorney's fees, costs, and expenses, including its investigation costs. Khandekar is further ENJOINED from using or disseminating, in any way, the trade secrets he reviewed without authorization at KCG between November 2016 and May 2017.

## **I. BACKGROUND**

### **A. KCG Hires Khandekar to Work on Predictors**

KCG is a financial-services firm. Chung Decl. ¶ 8. It “engages in propriety algorithmic trading and electronic market trading through exchanges and other computer-based platforms through the internet, in the United States and around the world.” Defendant’s Rule 56.1 Counterstatement (Def. 56.1 Ctr.), Dkt. No. 140, ¶ 1. In making its trading decisions, KCG relies on “predictive models that are designed to forecast price movements in securities markets.” *Id.* These models are called Predictors, and they are developed and refined by Quantitative Strategists, who are colloquially referred to as Quants. *Id.* ¶ 3. “Quants research various events, such as news, social media or trading volumes, to identify ‘signals’ that correlate to changes in market pricing, and they write source code that computes a predictive-market-based reaction to that signal.” *Id.* ¶ 4.

KCG’s predecessor firm hired Rohit Khandekar as a Quant in March 2012. *Id.* He was hired as part of the “signal team,” “a group of five or six Quants responsible for developing Predictors used in KCG’s customer market-making business.” Pl. Ex. 1, Khandekar Dep., 45:12-22; Def. Ctr. ¶ 5. Khandekar’s team included fellow Quant Evan Wright, and it was led by Steve Liu. Def. Ctr. ¶ 5. Liu in turn reported to Vladamir Neyman, co-head of KCG’s customer market-making business. *Id.* ¶¶ 6, 7. There were other teams of Quants at KCG. Def. Ctr. ¶ 8. Khandekar eventually became a “senior quant,” meaning he was “expected to come up with ideas for [his] projects on [his] own” and mentor junior team members. Khandekar Dep. 46:12-25.

Quants developed Predictors through coding. Codes for predictors consisted of two parts: The first part was “plumbing,” which dealt with nitty-gritty details like “injecting data, reading offline data, outputting certain things.” *Id.* 57:18-24. Khandekar described plumbing as

“the part of the source code that does all the peripheral things that a predictor has to do in order to work.” *Id.* 192:8-18. The second part was “the most valuable, and thus the most secret, part of the code” and was known as the Predictor’s “secret sauce.” Def. Ctr. ¶ 16. The secret sauce “contains the types of information, the combinations of information and the mathematical formulas that forecast future prices.” *Id.* Khandekar explained that the secret sauce “implements the core idea of the predictor” and governs “how [the Predictor] compute[s] those values, what values are computed and where they are stored, and how they are combined to compute an output value.” Khandekar Dep. 192:8-18. In other words, the secret sauce contains formulas that forecast future market prices, and thus permit KCG to make profitable trades.

#### **B. KCG’s Efforts at Secrecy**

Predictors are “some of KCG’s most-closely guarded confidential and proprietary trade secrets.” Plaintiff’s Rule 56.1 Counterstatement (Pl. 56.1 Ctr.), Dkt. No. 149, ¶ 43. KCG therefore took various efforts to maintain the secrecy of Predictors. First, there was a policy at KCG prohibiting Quants from sharing, with other Quants or employees, any details regarding the secret sauce of their Predictors. Khandekar stated that Quants “worked in silos to the extent that they cannot discuss the very details of the predictors that they are working on or the details of the projects they are working on.” Khandekar Dep. 94:8-11. He further stated that while he worked at KCG, he could not share “[t]he finer details” of the predictors he worked on. *Id.* 94:16-21. Quants thus could not discuss the secret sauce of predictors with one another. *Id.* 95:2-8. But KCG drew a line between secret sauce and plumbing. Khandekar made clear that Quants could “share tools, data, template predictors, for example, with other quants so as to -- so as to minimize the duplication of work.” *Id.* 94:12-15.

Wright explained that this policy operated like a sliding scale. The secret sauce could not be shared: “there is a general rule . . . that details specific to a predictor, exactly what the

calculation is are totally off limits.” Wright Dep. 97:5-10. But general concepts could: “Some aspects that are not specific to a single predictor are okay [to share] as concepts, if not as implementation.” *Id.* 97:11-13. And “in the gray area between that, you should ask [Neyman] or [Liu].” *Id.* 97:14-15. Khandekar’s manager, Liu, confirmed that discussions between Quants “regarding the work they were doing” were “only limited to high level ideas.” Liu Dep. 65:23-66:11; *see also id.* 67:14-19 (“we encourage collaboration, sharing, and brainstorming high-level research ideas.”).

Second, Quants used access restrictions to protect certain codes. KCG uses the Unix/Linux operating system to run its servers and computers. Def. Ctr. ¶ 24. In that system, “every file and every directory has ‘permissions’ that govern who can read, write or execute a file . . . Unix permissions can be set for the user, group (a collection of users) or everyone with Unix credentials (the ‘world.’)”. *Id.* Access permissions thus “enable a user to specifically authorize another user or group of users to access a directory or read or otherwise use a file.” Pl. Ctr. ¶ 51; *see also id.* ¶ 52. KCG instructs Quants “to create a default setting ensuring that no new directors and files have any group or other access permissions,” meaning that they should be accessible only to their creator. *Id.* ¶ 53.

Third, Quants use encryption to protect codes. *See* Pl. Ctr. ¶ 46 (“KCG Quants use two primary ways to restrict other KCG employees from electronically accessing confidential Predictor files: ‘encryption’ and ‘access permissions.’”). To understand how encryption works, some background is helpful: Quants develop and work on Predictors “in their personal directors within KCG’s servers.” Def. Ctr. ¶ 24; *see also* Pl. Ctr. ¶ 66 (“KCG also allocates every Quant specific space on the Linux system, to store his or her work-related directories and files.”). In order to access the secure servers containing Predictors, “an individual must have a valid Unix

login and password credentials.” Def. Ctr. ¶ 22. After a Quant completes a Predictor, she must encrypt its source code and check it into a source-code repository on the KCG servers.

“Encryption renders a file unreadable and un-editable unless someone has the required de-encryption ‘key’ which will enable them to unencrypt the file, and only in [its] unencrypted form [can they] read it or edit it.” Pl. Ctr. ¶ 47. When encrypting a Predictor, the Quant can input a list of authorized users, who will be “given the technical ability to decrypt the file.” Def. Ctr. ¶ 23. These other users are called “Additional PGP Recipients.” *Id.* The list of users on this list appears “in text at the top of the file.” *Id.* In other words, once a file is encrypted, only the individuals on this list are capable of decrypting and viewing its contents.

Another KCG employee, Philip Chung, testified that “predictors . . . were meant for only certain eyes only. And it was very explicit, because they all contained a line of text, which is additional PGP recipients, that lists those users that that file was meant for.” Chung Dep. 37:3-8; *see also id.* 114:9-12 (“There was very explicit intent for those files to be only accessible by the people listed on the additional PGP recipients line.”), 148:8-14. So long as the code is encrypted, “[i]ndividuals who are not listed as Additional PGP recipients cannot decrypt or view the secret code.” Def. Ctr. ¶ 23. “To work on a Predictor after the source code has been encrypted and committed to the [source-code repository,] a Quant with PGP credentials must download a copy of the encrypted code from the [repository] to his or her personal directory, and unencrypt the source code.” Def. Ctr. ¶ 24. However, if an authorized user unencrypts the source code and removes any access restrictions, then even users who are not listed on the authorized list can access and view its contents. Def. Ctr. ¶ 23. Even after decryption, the Recipients List still appears on the file. Pl. Ctr. ¶ 50.

Fourth, KCG instructed its Quants on how to protect sensitive information. For example, KCG promulgated instructions on “how to use secret servers . . . [and] how to typically put secret code into production” to all new Quants, and employees often referred back to these materials. Liu Dep. 80:14-81:19. Liu stated that “from time-to-time” he would “remind quants . . . to either use encryption or access restrictions to protect secret code that they were working on.” *See id.* 78:6-15; Def. Ctr. ¶ 26. KCG also “developed a number of informational pages for employees on how to set up their environment, protect source code with Unix permissions, and encrypt secret source code files in accordance with Company policy.” Def. Ctr. ¶ 26. Chung agreed that “it [was] KCG’s policy to require quants to restrict their directories” and testified that this policy was stated “various places on loop pages, on wiki pages, and certainly it [was] part of training for new quants.” Chung Dep. 75:4-12.

Fifth, Khandekar’s managers stopped Quants from sharing details regarding their Predictors. Khandekar stated that at several meetings “where quants went a little too far talking about specifics with their predictors,” “either [Neyman] or [Liu] stopped that quant from describing their predictor in more detail.” Khandekar Dep. 94:16-95:25. He explained that “in those other meetings, [Neyman] or [Liu] would say to the quant, ‘Hold off, we can talk about that outside of meeting.’” *Id.* Khandekar gave a specific example: at a “Friday weekly meeting,” various Quants were “together giving short updates on what they [had] done in the week or two weeks. And I believe it was [Wright] who was describing some of his work and was stopped by [Neyman.]” Khandekar Dep. 96:5-20. KCG admits to these facts without objection. Def. Ctr. ¶ 20.

Sixth, KCG required employees to sign employment agreements with confidentiality provisions. For example, Khandekar agreed in his employment agreement to “[h]old all

Confidential Information as a fiduciary in trust and use it only for the benefit of KCG in properly performing [his] employment duties for KCG” and to “[c]omply with KCG’s procedures on dealing with Confidential Information.” Pl. Ex. 12 (Employment Agreement), §§ 9(b), 11(b). These provisions are discussed at length below.

In sum, “KCG maintain[ed] a strong culture emphasizing the need to protect KCG’s confidential information, even against disclosure to other KCG Quants.” Pl. Ctr. ¶ 42. And it employed various tactics, ranging from policies against disclosure to contractual provisions, to effectuate that policy.

### **C. Khandekar Interviews with Two Sigma, and Reviews Other Quants’ Secret Sauce**

In October 2016, Two Sigma Securities, “one of KCG’s main competitors in signal research for market making, contacted Khandekar about an employment opportunity.” Def. Ctr. ¶ 32. Khandekar spoke with a friend at Two Sigma about the role. *Id.* A few weeks later, Khandekar submitted his resume to Two Sigma. *Id.* ¶ 35; Khandekar Dep. 131:21-24. On November 15, 2016, Khandekar’s friend shared his resume with Simon Yates, Two Sigma’s CEO. Yates was “super excited” by Khandekar’s application and viewed his candidacy as a “high priority.” Yates Dep. 25:14-26:7; Def. Ctr. ¶ 39. Khandekar was then asked to meet with Yates for breakfast in two weeks to discuss the opportunity. Khandekar Dep. 146:12-14, 19-21; Def. Ctr. ¶ 40.

In the time between learning of the breakfast meeting and the meeting itself, Khandekar accessed three of Evan Wright’s Predictors and reviewed them. Def. Ctr. ¶ 41. Wright had not access-restricted or otherwise encrypted these files, so they were available for other KCG employees, like Khandekar, to view. *Id.*

The breakfast meeting occurred as scheduled, and that same day Two Sigma invited Khandekar for an in-person interview. On December 15, 2016, Khandekar interviewed with various Two Sigma employees. Def. Ctr. ¶ 44. Following the interview, Yates and Two Sigma began formulating how to negotiate an offer for Khandekar. Def. Ctr. ¶ 45.

Between December 28 and 30, 2016, “Khandekar ran seven custom ‘scripts’ to search and filter other Quants’ directories for unencrypted source code files.” Def. Ctr. ¶ 46. In other words, Khandekar designed a code to search other Quants’ storage for unencrypted files, including Predictors. *Id.* Indeed, he admitted that he was “specifically searching for unencrypted predictors.” Khandekar Dep. 182:6-8. Within his own personal directory, Khandekar then created multiple folders named after other Quants. Def. Ctr. ¶ 48 (“Khandekar created . . . multiple subdirectories named after other Quants, based on their usernames” such as “Evan Wright (ewright)”). These folders included the names of Quants who were and were not on Khandekar’s team. *Id.* Khandekar then copied “at least 160 source code files from these Quants’ directories into the corresponding” folders he had created. *Id.* ¶ 49. Khandekar stated that these files were “very close to the ones in production [at KCG] in terms of functionality” and that “the secret sauce from these files also was very similar to the ones in production.” Khandekar Dep. 185:13-188:17. Khandekar was not listed as an Additional PGP Recipient for any of these source-code files. Def. Ctr. ¶ 50.

On January 6, 2017, Yates and Khandekar had a “long call” about his candidacy. Def. Ctr. ¶ 54. Khandekar then left for a vacation. *Id.* ¶ 55. While on that vacation and for a time after, Khandekar reviewed the Predictors he had copied, some on multiple occasions. Def. Ctr. ¶ 56. And he began “methodically sorting Predictors as he reviewed them” in his own directory. *Id.* ¶ 57. He created additional folders, including ones titled “done” and “good.” *Id.* For



example, Khandekar opened and read three of a fellow Quant's Predictors, and then moved them into a "done" subfolder in his folder for that Quant. *Id.* ¶ 57. He also "moved at least six files to the two 'good' folders." *Id.* ¶ 59.

On February 16, 2017, Two Sigma offered Khandekar a Quant position. *Id.* ¶ 63. Over the next weeks, Khandekar negotiated the terms of his offer. *Id.* ¶ 65. And at the same time, he continued to review other Quants' source code files, including two developed by Evan Wright. *Id.* ¶¶ 63, 70. Two Sigma eventually increased the compensation in the offer. *Id.* ¶ 66. On March 6, 2017, Khandekar removed and deleted all 160 source-code files he had copied from other users' directories. *Id.* ¶ 68. On March 14, 2017, he signed Two Sigma's revised offer letter, and he soon left KCG. *Id.* ¶¶ 69, 77.

In April 2017, KCG was investigating the theft of trade secrets by another employee. In connection with that investigation, KCG discovered that Khandekar had copied other Quants' Predictors into his personal directory. *Id.* ¶ 78. It soon initiated this lawsuit. *Id.* ¶ 79. In June 2017, Two Sigma withdrew its offer of employment. Pl. Ctr. ¶ 28.

#### **D. Procedural History**

On May 11, 2017, KCG filed suit against Khandekar alleging misappropriation of trade secrets in violation of federal and state law and breach of contract. It sought a temporary restraining order, which the Court denied. *See* Dkt. No. 26, Ex. 1; Dkt. No. 9 at 8:19-20. On June 22, 2017, KCG filed a motion for a preliminary injunction to, among other things, enjoin Khandekar from using or accessing its confidential information. *See* Dkt. No. 24. The parties resolved that motion by entering a joint stipulation on July 5, 2017. *See* Dkt. No. 39. On January 18, 2018, the Court stayed this action pending resolution of an arbitration. Dkt. No. 141. That arbitration was dismissed and the stay was vacated on February 20, 2018. Dkt. No. 144. The parties then cross-moved for summary judgment. That motion is now before the Court.

## II. SUMMARY JUDGMENT STANDARD

“Summary judgment is appropriate when the record taken as a whole could not lead a rational trier of fact to find for the non-moving party.” *Smith v. Cty. of Suffolk*, 776 F.3d 114, 121 (2d Cir. 2015). Summary judgment may not be granted unless all of the submissions taken together “show[] that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(a). The moving party bears the burden of demonstrating the absence of a material factual question, and in making this determination, the Court must view all facts in the light most favorable to the non-moving party. See *Eastman Kodak Co. v. Image Techn. Servs., Inc.*, 504 U.S. 451, 456 (1992); *Gemmink v. Jay Peak Inc.*, 807 F.3d 46, 48 (2d Cir. 2015). In evaluating cross-motions for summary judgment, each motion must be examined “on its own merits,” and “all reasonable inferences must be drawn against the party whose motion is under consideration.” *Vugo, Inc. v. City of New York*, 931 F.3d 42, 48 (2d Cir. 2019).

Once the moving party has asserted facts showing that the non-movant’s claims cannot be sustained, “the party opposing summary judgment may not merely rest on the allegations or denials of his pleading; rather his response, by affidavits or otherwise as provided in the Rule, must set forth specific facts demonstrating that there is a genuine issue for trial.” *Wright v. Goord*, 554 F.3d 255, 266 (2d Cir. 2009). “[C]onclusory statements, conjecture, and inadmissible evidence are insufficient to defeat summary judgment.” *Ridinger v. Dow Jones & Co. Inc.*, 651 F.3d 309, 317 (2d Cir. 2011). The same is true for “mere speculation or conjecture as to the true nature of the facts.” *Hicks v. Baines*, 593 F.3d 159, 166 (2d Cir. 2010). And “[w]hen opposing parties tell two different stories, one of which is blatantly contradicted by the record, so that no reasonable jury could believe it, a court should not adopt that version of the

facts for purposes of ruling on a motion for summary judgment.” *Scott v. Harris*, 550 U.S. 372, 380 (2007).

Only disputes over material facts will properly preclude the entry of summary judgment. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). “An issue of fact is genuine and material if the evidence is such that a reasonable jury could return a verdict for the nonmoving party.” *Cross Commerce Media, Inc. v. Collective, Inc.*, 841 F.3d 155, 162 (2d Cir. 2016). “On a motion for summary judgment, a fact is material if it might affect the outcome of the suit under the governing law.” *Royal Crown Day Care LLC v. Dep’t of Health & Mental Hygiene*, 746 F.3d 538, 544 (2d Cir. 2014) (internal quotation marks omitted).

### **III. KHANDAKAR BREACHED MULTIPLE TERMS OF HIS EMPLOYMENT AGREEMENT WITH KCG**

Khandekar’s Employment Agreement states that it “shall be governed by and interpreted in accordance with New Jersey law (without regard to its conflict of law rules).” Employment Agreement § 13(e). The parties agree that New Jersey law applies to the breach-of-contract claims in this case. To state a claim for breach of contract in New Jersey, a plaintiff must show that (1) the parties entered into a valid contract; (2) the defendant failed to perform his duties under the contract; and (3) the plaintiff sustained damages as a result of the breach. *Lincoln Harbor Enterprises, LLC v. M.Y. Diplomat*, 2008 WL 5046787, at \*5 (D.N.J. Nov. 21, 2008) (citing *Murphy v. Implicito*, 392 N.J. Super. 245, 920 A.2d 678, 689 (N.J. Super. Ct. App. Div. 2007)). The parties do not dispute the validity of the Employment Agreement. The Court must therefore determine whether Khandekar failed to perform his contractual duties. The Court concludes that there is no genuine dispute of material fact that he did, in two ways.

### **A. Khandekar Breached His Employment Agreement By Reviewing the Secret Sauce of Predictors He Did Not Work On**

Khandekar's Employment Agreement contains multiple provisions creating duties regarding confidential information. Three are relevant here:

- Section 3(c) obligated Khandekar to "Act in an honest and ethical manner in compliance with all applicable laws, ordinances, permits, licenses, governmental rules, regulations, authorizations and requirements, and comply with the policies, procedures, requirements, rules and regulations in effect at any time by KCG, any exchange, regulatory agency or self-regulatory body with authority to govern or regulate [him] or KCG."
- Section 9(b) obligated Khandekar to "(i) Hold all Confidential Information as a fiduciary in trust and use in only for the benefit of KCG in properly performing [his] employment duties for KCG; (ii) Maintain Confidential Information in strict confidence and secrecy; (iii) Not, except as specifically directed by KCG in performing [his] employment duties for KCG, communicate or disclose Confidential Information in any manner to any person within or outside KCG who is not authorized to know, use or receive such Confidential Information; and (iv) Comply with KCG's procedures on dealing with Confidential Information and in all events use [his] best efforts to prevent the inadvertent disclosure of Confidential Information."
- Section 11(b) obligated Khandekar to "not use [KCG's] systems and software for personal purposes contrary to KCG's interests" and to "not use a code, access a file or retrieve any stored communication, other than as authorized by KCG to perform [his] job duties, without prior clearance from KCG."

As discussed above, KCG had a policy prohibiting Quants from learning the secret sauce of Predictors they did not work on. Khandekar himself repeatedly discussed the policy. For example, he testified that KCG had about 100 predictors during his employment. Khandekar developed and worked on about 10 of those 100. Pl. Ctr. ¶ 1; Khandekar Dep. 137:2-9. Khandekar agreed that “[he] should not have had knowledge of the secret sauce for [the remaining] 90 percent of the predictors . . . at KCG.” *Id.* 137:6-11. And he said that he “understood that KCG intentionally walled [him off] from knowing the secret sauce of the predictors that [he] did not personally develop.” *Id.* 137:13-17. He also explained the converse of this rule: “[his] fellow quants should not know the secret sauce of the 10 percent or so of predictors that [he] developed.” *Id.* 137:18-25.

Other Quants testified to this policy as well. To take one example, Wright stated that “there [was] a general rule . . . that details specific to a predictor, exactly what the calculation [in the predictor] is are totally off limits.” Wright Dep. 97:5-10. Even though this rule “was not written down,” it was known to KCG’s employees, including Khandekar. *Id.* 97:20. There is no genuine dispute that KCG prohibited Quants from knowing the secret sauce of Predictors which they were not responsible for.

The undisputed facts demonstrate that Khandekar violated this policy, over a period of multiple months, by copying and reviewing entire Predictors developed by other Quants. Khandekar admits that he accessed entire Predictors of other Quants. Khandekar Decl. ¶¶ 35, 39. Those files contained secret sauce, and Khandekar thus learned sensitive information about Predictors that he had no role in developing.

Khandekar was also not listed as an Authorized PGP Recipient for those source-code files, further confirming that he was not authorized to view them. KCG employees agree that the

PGP list is “a very explicit authorization mechanism” that lists the *only* employees who are permitted to view and access certain code. Chung Dep. 106:3-5. But Khandekar was not listed as an Additional PGP Recipient on *any* of the 160 source-code files he copied into his directory. Def. Ctr. ¶ 50. Nor did Khandekar’s supervisors, Liu and Neyman, give him direct permission to access these files. *Id.*

By violating this policy, Khandekar breached all three of the contractual provisions governing confidentiality. He did not comply with the “rules and regulations in effect at any time by KCG.” Employment Agreement Section 3(c). He did not “[c]omply with KCG’s procedures on dealing with Confidential Information.” *Id.* § 9(b)(iv). And he “access[ed] a file . . . other than as authorized by KCG to perform [his] job duties, without prior clearance from KCG.” *Id.* § 11(b). He thus breached these three provisions of the Employment Agreement.

Khandekar makes several arguments to excuse this breach, but none succeeds. First, Khandekar repeatedly argues that the files he copied and viewed did not have access restrictions and were not encrypted. Def. Br. at 10. Second, Khandekar notes that he accessed the files using his proper work login. *Id.*; *see also* Chung Dep. 97:11-18 (agreeing that Khandekar “hadn’t logged on [to KCG’s computer network] using anything other than his credentials.”); Pl. Ctr. ¶ 86 (parties agreeing to this fact). Third, Khandekar points out that this policy was unwritten. He claims that “KCG did not have any written policy prohibiting Quants from accessing and viewing decrypted files for which they were not listed on the file’s Additional PGP Recipients” or “from accessing the personal workspace on the Linux System allocated to other Quants.” Pl. Ctr. ¶¶ 39, 40.

All three of Khandekar’s arguments do fail for the same reason: KCG had an unwritten policy prohibiting Quants from viewing each other’s secret sauce. As noted, there is no genuine

dispute that KCG had an unwritten policy against Khandekar's behavior. Khandekar, Wright, and Liu all testified that Quants were prohibited from viewing each other's secret sauce. This is why, for example, Khandekar's supervisors cut off Quants in multiple conversations who verged too close to sharing sensitive details. And Wright made clear that this policy "was not written down," but nonetheless was in place at KCG and "was [not] just [his] sense" of how things at KCG worked. Wright Dep. 97:17-25. Khandekar provides no evidence rebutting these statements from several KCG employees regarding the prohibition on Quants sharing secret sauce with one another. Once again, his own testimony confirms as much. Khandekar stated expressly that he "could not discuss the secret sauce and [his] predictors with [his] fellow quants," and that those Quants "could not discuss the secret sauce of their predictors with [him.]" Khandekar Dep. 94:16-95:8; Def. Ctr. ¶ 18. And Khandekar presents no legal reason why a policy like this one must be written down to have force. It does not matter, therefore, that the Quants whose files Khandekar viewed failed to put in place access restrictions on the relevant files. And it also does not matter that Khandekar was properly logged onto KCG's servers using his valid credentials. Restrictions or not, authorized login or not, KCG's policy made clear that Khandekar had no authority to view these files.

Khandekar last argues that KCG lacks standing to pursue this claim because it cannot demonstrate damages. But KCG's injury in fact is the multiple breaches of the Employment Agreement. And as discussed below, KCG is entitled to damages here.

In short, the undisputed record establishes that Khandekar did not have any authorization to look at the files he reviewed between November 2016 and February 2017. He therefore violated the terms of his Employment Agreement by doing so.

### **B. Khandekar Also Breached the Employment Agreement by Deleting Files**

Those are not the only provisions of the Employment Agreement that the undisputed record establishes were breached by Khandekar. Section 11(a) of the Agreement states:

Upon termination of my employment (regardless of the reason) and at any other time at KCG's request, I will immediately deliver to KCG, or (if requested by KCG) destroy or permanently erase, all of KCG's property, including documents, handwritten notes, computer and physical files, records of developments, keys and key cards, access codes, credit cards, tapes, disks and other electronic, optical, magnetic or other media, and all other KCG property in my possession or control (whether or not it contains, refers to or was derived from Confidential Information).

The parties agree that on Khandekar's last day at KCG, he turned in his work-issued laptop after he himself "wiped it clean." Khandekar Dep. 240:17-20. He argues that he wiped it clean because he "didn't know any way of" securely deleting his personal information from the laptop while leaving KCG's information in place. *Id.* at 242:3-6; *see also* Def. Ctr. ¶ 77. The Employment Agreement is clear, however, that Khandekar can "[d]estroy or permanently erase" KCG's electronic files only "if requested by KCG." § 11(a). In the absence of such a request, Khandekar was obligated to deliver the electronic property to KCG. Khandekar therefore violated this provision of the Employment Agreement.

Khandekar argues that other employees had also deleted files in this manner. Def. Br. 29-30. But he provides no authority under New Jersey law for the proposition that the breach of a similar contract by a non-party provides any defense. The undisputed record thus demonstrates that Khandekar also violated the Employment Agreement by wiping his work-issued laptop without KCG's permission.

### **C. Pursuant to the Employment Agreement, KCG is Entitled to Attorney's Fees and Expenses, Including its Investigative Costs**

The Employment Agreement also shifts certain fees and costs to Khandekar in the event of a breach. It states:



If [Khandekar] [is] found to be in breach or default in the full or timely performance of any of [his] covenants, duties or obligations as set forth in this Agreement, [he] will be liable for, and agree to promptly pay to KCG upon demand, all of the costs and expenses KCG incurs as a result of or arising from such breach or default, including, reasonable attorneys' fees and expenses and court costs.

Employment Agreement § 13(d).

The Court has found Khandekar in breach of multiple contractual duties under the Agreement. The contract's clear terms therefore mandate that Khandekar pay "*all of the costs and expenses KCG incurs as a result of or arising from such breach.*" *Id.* (emphasis added). Khandekar must therefore pay KCG's attorney's fees. Moreover, KCG retained a third party to investigate Khandekar's activities. Def. Ctr. ¶ 79. KCG paid \$194,382.28 for that investigation. *Id.* And that investigation was "incur[ed] as a result of or arising from" Khandekar's breach of the Employment Agreement. Indeed, Khandekar admits that KCG retained this third party to investigate his conduct. *Id.* Khandekar is therefore obligated to pay for the investigation.

Khandekar argues that this "one-way attorneys' fees provision is . . . unconscionable and therefore unenforceable." Def. Br. at 31. For a claim of contract unconscionability under New Jersey law, the Court must "determine whether the contract is so oppressive, or inconsistent with the vindication of public policy, that it would be unconscionable to permit its enforcement." *Rodriguez v. Raymours Furniture Co.*, 225 N.J. 343, 367 (2016) (internal quotation marks omitted). Unconscionability may be either substantive or procedural. Procedural unconscionability refers to unfairness in the formation of the contract, and may be shown by "a variety of inadequacies, such as age, literacy, lack of sophistication, hidden or unduly complex contract terms, bargaining tactics, and the particular setting existing during the contract formation process." *Muhammad v. Cty. Bank of Rehoboth Beach, Del.*, 189 N.J. 1, 912 A.2d 88, 96 (2006) (internal quotation marks omitted). A contract term may also be substantively

unconscionable if it is “‘excessively disproportionate’ and involves an “‘exchange of obligations so one-sided as to shock the court’s conscience.’” *Delta Funding Corp. v. Harris*, 189 N.J. 28, 912 A.2d 104, 120 (2006) (quoting *Sitogum Holdings, Inc. v. Ropes*, 352 N.J. Super. 555, 800 A.2d 915, 921 (N.J. Super. Ct. Chanc. Div. 2002)).

To start, Khandekar points to no evidence of procedural unconscionability in the contract’s formation. He instead raises a bare assertion that his Employment Agreement is a contract of adhesion and therefore unenforceable. But equal bargaining power between parties is not a prerequisite to contractual validity. *See Argabright v. Rheem Mfg. Co.*, 201 F. Supp. 3d 578, 596 (D.N.J. 2016). Nothing suggests that Khandekar had so little bargaining power and control over the terms of his Employment Agreement that it was one of adhesion. And he presents no evidence that the contract was “presented in a take-it-or-leave-it basis” or in a “standardized printed form.” *Estate of Ruszala ex rel Mizerak v. Brookdale Living Communities, Inc.*, 415 N.J. Super. 272, 294 (N.J. App. Div. 2010). Khandekar does not explain why he could not have simply refused to accept his original offer of employment. Nor does the Court find this term so disproportionate as to be substantively unconscionable; although it exposes Khandekar to significant liability, fee-shifting is a common feature of modern contracts. Indeed, courts have found such contracts enforceable under New Jersey law. In *Allia v. Target Corp.*, Target asserted a breach-of-contract counterclaim against the plaintiff for violating a confidentiality agreement. 2010 WL 1050043, \*12 (D.N.J. 2010). The Court found that the plaintiff had breached the contract. *Id.* at \*14. The contract also provided that “Target Corporation shall be entitled, in addition to any other remedies available, to injunctive and/or equitable relief to prevent a breach of this Agreement or any part of it, and reasonable attorney’s fees in enforcing

this Agreement.” *Id.* The Court thus granted fees to Target, despite the vastly different bargaining power between the two parties and potential for large liability. *Id.* at \*15.

The same is true here. The Employment Agreement clearly requires Khandekar to pay any costs and expenses incurred by KCG due to a contractual breach. KCG has incurred attorney’s fees and investigative costs, and Khandekar is obligated to pay them.

#### **IV. KCG IS ENTITLED TO SUMMARY JUDGMENT ON KHANDEKAR’S BREACH-OF-CONTRACT CLAIM**

Khandekar also asserts a breach-of-contract counterclaim against KCG. The Employment Agreement requires Khandekar not to compete with KCG for six months after ending his employment. Employment Agreement § 6(a). It further provides for KCG to pay Khandekar non-compete payments during this time, including six months of his annual salary. *Id.* § 6(b). Khandekar claims that KCG has breached this obligation by not paying him these payments for a full six months.

Khandekar’s argument fails. The Employment Agreement provides that “[n]on-compete payments will stop if KCG determines that [Khandekar] [has] violated any provision of this Agreement.” *Id.* As discussed, Khandekar has breached multiple terms of his employment contract, and KCG discovered these violations in May 2017. KCG paid Khandekar some non-compete payments, Pl. Ctr. ¶¶ 11-12, but it had no further duty to do so once it discovered his breach. The Court thus rejects Khandekar’s contractual counterclaim as a matter of law.

#### **V. KHANDEKAR VIOLATED THE DEFEND TRADE SECRETS ACT**

KCG next argues that Khandekar violated the federal trade-secrets statute. The Defend Trade Secrets Act (DTSA) provides a private cause of action to the “owner of a trade secret that is misappropriated.” 18 U.S.C. § 1836(b)(1). The parties do not dispute that KCG’s Predictors are trade secrets. Def. Ctr. ¶¶ 16, 17 (parties agree that “the entire source code of a predictor is

considered trade secret information and extremely valuable intellectual property.”); *see generally ExpertConnect, L.L.C. v. Fowler*, 2019 WL 3004161, at \*4 (S.D.N.Y. July 10, 2019) (explaining requirements for information to constitute a trade secret under the DTSA). The parties also do not dispute that the Predictors are used in trading around the United States and the world, and thus satisfy the DTSA’s interstate-commerce requirement. *See United States v. Agarwal*, 726 F.3d 235, 244-51 (2d Cir. 2013) (holding that computer code used for securities trading satisfied the interstate commerce requirement because “the confidential code was valuable only in relation to the securities whose interstate trades it facilitated.”).

This claim therefore boils down to whether Khandekar *misappropriated* KCG’s trade secrets. The DTSA defines “misappropriation” to include “acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means” or “disclosure or use of a trade secret of another without express or implied consent” in specified circumstances.” 18 U.S.C. § 1839(5). The statute thus “contemplates three theories of liability: (1) acquisition, (2) disclosure, or (3) use.” *Opternative, Inc. v. JAND, Inc.*, 2019 WL 624853, at \*6 (S.D.N.Y. Feb. 13, 2019) (internal quotation marks and citation omitted). Because the undisputed record establishes that Khandekar both acquired and used KCG’s trade secrets, he misappropriated them, and KCG is therefore entitled to summary judgment on its DTSA claim.

#### **A. Khandekar Improperly Acquired KCG’s Trade Secrets**

KCG argues that Khandekar improperly acquired its trade secrets. Many of the statutory requirements for misappropriation are met: Khandekar *acquired* trade secrets by copying Predictors from other Quants’ repositories into his own. Those trade secrets *belonged to another person*, KCG. *See* 18 U.S.C. § 1839(5).

The parties dispute whether Khandekar used *improper means* to acquire the data. *See id.* The undisputed facts establish that he did. The DTSA states “the term improper means . . . includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means.” *Id.* § 1839(6). Khandekar raises a now-familiar argument: the files he copied were not access restricted or encrypted, and thus his actions were not improper. Khandekar’s actions however meet one of the enumerated examples in this list: he breached a duty to maintain secrecy. As discussed, Khandekar breached multiple confidentiality provisions of his Employment Agreement. For example, he had an obligation “not use a code, access a file or retrieve any stored communication, other than as authorized by KCG to perform [his] job duties, without prior clearance from KCG.” Employment Agreement § 9(b). Because he violated that duty, his acquisition was accomplished using improper means.

Even in the absence of these contractual provisions, Khandekar’s actions constitute improper means. The DTSA makes clear that its definition of improper means is non-exhaustive, and other facts may suffice. The undisputed record establishes that Khandekar knowingly violated KCG’s policy prohibiting him from accessing Predictors developed by other Quants. The Court concludes that knowingly procuring confidential data of others, in violation of an employer’s policy, by itself satisfies the improper-means requirement.

Finally, Khandekar had *actual knowledge*—or at the very least, constructive knowledge—of the fact that the trade secret was acquired by these improper means. He was familiar with KCG’s policy; he explained it himself at length in his deposition. *See* Khandekar Dep. 137:2-25. And he copied the files himself and organized them into various directories. This satisfies the knowledge requirement. In short, the undisputed record establishes that

Khandekar improperly acquired and therefore misappropriated KCG's trade secrets, thereby violating the DTSA.

### **B. Khandekar Improperly Used KCG's Trade Secrets**

KCG also argues that Khandekar misappropriated its trade secrets through use. KCG must tick three statutory boxes to succeed on this theory. Khandekar must have "used improper means to acquire knowledge of the trade secret." 18 U.S.C. § 1839(5)(B)(ii)(I). For the same reasons as above, this requirement is met here as a matter of law. Khandekar must also have lacked "express or implied consent" from KCG. *Id.* § 1839(5)(B). Once again, KCG had a policy clearly prohibiting Khandekar's actions. That leaves one statutory requirement: Khandekar must have *used* the trade secret. The Court concludes that there is no dispute that this requirement is met, and KCG is thus entitled to summary judgment on this issue.

There is no dispute that Khandekar copied, viewed, and organized Predictors developed by his fellow Quants. To reiterate, Khandekar admits that he copied 160 source-code files from other Quants' directories, placed those files into his own personal directory, reviewed most of them (sometimes several times each), organized them into folders in part based on how "good" they were, and then deleted the files. He says he had a legitimate reason behind doing so: he accessed the Predictors to increase his knowledge base and thus create better Predictors for KCG. For example, he says he "was working on a Predictor for KCG based on 'book data,'" and thus wanted to learn how other Quants had approached the topic. Def. Br. at 11-12; Def. Ctr. ¶ 41. Order-book pressure is "the relative balance of limit orders to buy or sell that reside on the order books of stock exchanges." Def. Ctr. ¶ 31. In his declaration, Khandekar explained that he "was unfamiliar with how to inject book data effectively into a Predictor implementation since this was the first time [he] was developing a Predictor that worked with book data." Khandekar Decl. ¶ 34. He then stated that "he needed to find some template or sample Predictors to learn

how that implementation was done.” *Id.* ¶ 35. In short, Khandekar “believed the source code files were potentially useful in the work he was doing for KCG.” Def. Ctr. ¶ 49; *see also id.* ¶ 51 (“In fact, Khandekar had accessed those source code files for his Predictor research and implementation work at KCG for the benefit of KCG.”). He claims that he “accessed the files *only* in furtherance of [his] work for KCG.” Khandekar Decl. ¶ 39 (emphasis in original). Khandekar’s purported motive, however, is irrelevant. Reviewing another’s trade secrets to develop one’s personal knowledge constitutes use, and therefore misappropriation—even if that review is ostensibly for the trade secret owner’s benefit. The Court reaches this conclusion based on three rationales.

*First*, the Court begins, as it must, with the statute’s text. *See Caraco Pharm. Labs., Ltd. v. Novo Nordisk A/S*, 566 U.S. 399, 412 (2012) (“We begin where all such inquiries must begin: with the language of the statute itself.”). The DTSA defines “misappropriation” as “use of a trade secret of another without express or implied consent by a person who . . . used improper means to acquire knowledge of the trade secret.” 18 U.S.C. § 1839(5). Although the statute provides several definitions, such as for improper means, it does not provide one for use. The Court thus turns to dictionary definitions of the term. Black’s Law Dictionary defines “use” as “[t]o employ for the accomplishment of a purpose; to avail oneself of.” Black’s Law Dictionary, “Use” (11th ed. 2019). Merriam-Webster defines the verb as “to put into action or service[;] avail oneself of.” Merriam-Webster Dictionary, “Use,” *available at* <https://www.merriam-webster.com/dictionary/use>. And the Oxford English Dictionary defines “use” as “[t]he act of putting something to work, or employing or applying a thing, for any (esp. a beneficial or productive) purpose; the fact, state, or condition of being put to work, employed, or applied in

this way; utilization or appropriation, esp. in order to achieve an end or pursue one's purpose.”

Oxford English Dictionary, “Use,” *available at* <https://www.oed.com/view/Entry/220635>.

Khandekar’s actions tick all these boxes. He admits that he viewed other Quants’ Predictors to increase his knowledge and produce better work product. He thus employed that information to accomplish a purpose. He availed himself of that information. He put it to work for a productive purpose. Under any of the above definitions, Khandekar’s actions constitute “use” of KCG’s trade secrets.

Khandekar attempts to evade this plain reading by arguing that his “use” was benevolent: he was reviewing these files only to produce more profitable Predictors. But that argument does not allow him to escape the statute’s plain meaning. Irrespective of whether his actions were intended to benefit KCG, he still put the other Quants’ trade secrets to work for some purpose.

It is also undisputed that Khandekar’s use was not exclusively to KCG’s benefit. Even if it allowed him to develop more profitable Predictors, he was still compensated in part based on his performance at work. Producing better Predictors thus did not just benefit KCG—it directly and materially benefited him. Finally, even accepting Khandekar’s theory, the Court still rejects his argument. Assume that there is a direct correlation between review of KCG’s Predictors and a Quant’s performance. On this theory, the more Predictors a Quant reviews, the better she performs. That does not permit Khandekar—or any Quant—to unilaterally conclude that violating KCG’s policies is in fact in the firm’s best interest. Indeed, KCG concedes that “[i]t may be true that if KCG’s Quants had been provided with permission to view each other’s secret source code, it could conceivably have resulted in better, more profitable Predictors for KCG.” Pl. Br. at 12. But KCG had to weigh that potential benefit against other interests: “However, that would have put all of KCG’s most valuable trade secrets at risk every time a Quant left the



company.” *Id.* The undisputed evidence establishes that KCG struck a balance between these competing interests by deciding that Quants could review only their own Predictors and only discuss high-level concepts with one another. Khandekar cannot violate that policy and then escape the consequences by claiming that he did so for KCG’s benefit, when KCG itself has foregone any such benefit.

*Second*, the Court turns to the Restatement (Third) of Unfair Competition. The Restatement provides: “There are no technical limitations on the nature of the conduct that constitutes ‘use’ of a trade secret . . . As a general matter, any exploitation of the trade secret that is likely to result in injury to the trade secret owner or enrichment to the defendant is a ‘use.’” Restatement (Third) of Unfair Competition § 40 cmt. c (Am. Law. Inst. 1995). The Restatement then provides a non-exhaustive list of examples constituting use: “marketing goods that embody the trade secret, employing the trade secret in manufacturing or production, relying on the trade secret to assist or accelerate research or development, or soliciting customers through the use of information that is a trade secret.” *Id.* The Reporters’ Note further elaborates that use in trade-secrets law “is not limited to the sale of goods embodying or produced by means of the trade secret.” *Id.* Reporters Notes cmt. c.

Courts in this District have repeatedly looked to the Third Restatement, and this comment in particular, for guidance in interpreting the DTSA and its state-law equivalents. *See, e.g., Next Commc’ns, Inc. v. Viber Media, Inc.*, 2016 WL 1275659, at \*4 (S.D.N.Y. 2016); *Advanced Analytics, Inc. v. Citigroup Glob. Mkts, Inc.*, 2009 WL 7133660, at \*17 (S.D.N.Y. 2009) (adopting Restatement definition of “use”), *report and recommendation adopted in part, rejected in part*, 2010 WL 4780772 (S.D.N.Y. 2010); *Saniteq, LLC v. GE Infrastructure Sensing, Inc.*, 2018 WL 4522107, at \*1 (E.D.N.Y. 2018), *report and recommendation adopted*, 2018 WL

4357475 (E.D.N.Y. 2018). Courts of Appeals around the country have done the same. *See Wellogix, Inc. v. Accenture, L.L.P.*, 716 F.3d 867, 877 (5th Cir. 2013); *JustMed, Inc. v. Byce*, 600 F.3d 1118, 1130 (9th Cir. 2010); *Learning Curve Toys, Inc. v. PlayWood Toys, Inc.*, 342 F.3d 714, 728 (7th Cir. 2003).

Once again, there is no dispute that Khandekar's conduct meets the bill. He exploited KCG's trade secrets—other Quants' Predictors, including their secret sauce—for his own enrichment. He admits that he used the trade secrets to increase his own knowledge and skills. And his enrichment also included potential financial benefits; as discussed above, his compensation was tied to the profitability of his work for the firm. He thus used KCG's trade secrets within the meaning of the Restatement.

*Third*, Khandekar cites inapt caselaw and advances unavailing arguments in response to KCG's position. Khandekar points to *Jasmine Networks, Inc. v. Marvell Semiconductor, Inc.*, where the alleged appropriator merely "engaged in a conversation . . . about a hypothetical situation about the potential legal implications of using [the plaintiff's] trade secrets." 2013 WL 3776188, at \*13 (Cal. Ct. App. July 17, 2013). The Court held that "[a] discussion, in generic terms, of a company possessing a trade secret" does not constitute use. *Id.* \*40. Here, Khandekar did not merely discuss possession of a trade secret. Instead, he relied on that trade secret to develop his knowledge and expertise. The defendant in *Jasmine* did not engage in any such conduct. Khandekar also argues that the Court's holding will "effectively impose a gag order on employees discussing their relevant work experience during a search for employment." Def. Br. at 23. He goes on to claim that "KCG's claim of improper use applies equally to any discussion about the Predictors that Khandekar personally developed." *Id.* The Court rejects this argument. Khandekar did not violate the DTSA by gaining knowledge about trade secrets he

worked on, because he did not acquire them through improper means. And the Court does not rely on Khandekar's representations to Two Sigma in his resume or in his interviews to find a DTSA violation.

To be sure, Khandekar is correct that this case touches on “the outer reaches of the definition of ‘use’ under the DTSA.” Def Br. at 22. The Court has found no case directly applying “use” under the DTSA, or its state-law equivalents, to this sort of theory. But courts around the country have recognized that “use” in the Restatement and in trade-secrets law generally is a “very broad concept.” *Cognis Corp. v. CHEMCENTRAL Corp.*, 430 F. Supp. 2d 806, 812 (N.D. Ill. 2006); *accord* *BladeRoom Grp. Ltd. v. Emerson Elec. Co.*, 331 F. Supp. 3d 977, 986–87 (N.D. Cal. 2018). This would be a different case if Khandekar had merely copied the Predictors into his personal directory and done nothing more. Yet Khandekar admits—repeatedly—to using the Predictors to increase his personal knowledge. He thus improperly used KCG's trade secrets, and therefore misappropriated them under the DTSA.<sup>1</sup> Khandekar thus violated the DTSA both by improper acquisition and improper use.

### **C. The Court Need Not Decide Whether KCG is Entitled to Fees**

The DTSA provides that “if . . . the trade secret was willfully and maliciously misappropriated” a court may award “reasonable attorney's fees to the prevailing party.” 18 U.S.C. § 1836. Because the Court has already awarded KCG attorney's fees under the Employment Agreement, it need not decide whether KCG is also entitled to them under the DTSA.

---

<sup>1</sup> Because the Court concludes that Khandekar used KCG's trade secrets by learning from them, it does not address KCG's alternative argument that Khandekar used its trade secrets by misrepresenting to Two Sigma that he had experience working on Predictors based on order-book pressure.

#### **D. Khandekar Is Not Entitled to Fees**

Khandekar also seeks “reasonable attorneys’ fees in connection with defending this action under 18 USC 1836(b)(3)(D) and/or Federal Rule of Civil Procedure 11.” Defendant’s Amended Answer, Dkt. No. 90, ¶ 169. The DTSA provides that a court may award fees “if a claim of the misappropriation is made in bad faith, which may be established by circumstantial evidence.” 18 U.S.C. § 1836(b)(3)(D). Khandekar presents no evidence, circumstantial or otherwise, that KCG brought this claim in bad faith. To the contrary, KCG has prevailed in showing two independent violations of the DTSA. Similarly, Khandekar presents no argument or evidence warranting Rule 11 sanctions here. The Court therefore denies his counterclaim for fees.

#### **VI. KHANDEKAR ALSO VIOLATED NEW YORK STATE TRADE SECRETS LAW**

KCG next argues that Khandekar violated New York’s common law governing trade secrets. To succeed on a misappropriation of trade secrets claim under New York law, a party must demonstrate “(1) that it possessed a trade secret, and (2) that the defendants used that trade secret in breach of an agreement, confidential relationship or duty, or as the result of discovery by improper means.” *E.J. Brooks Co. v. Cambridge Sec. Seals*, 31 N.Y.3d 441, 452, 105 N.E.3d 301, 310 (2018) (internal quotation marks and citation omitted); *accord Faiveley Transp. Malmö AB v. Wabtec Corp.*, 559 F.3d 110, 117 (2d Cir. 2009); *Elsevier Inc. v. Doctor Evidence, LLC*, 2018 WL 557906, at \*2-3, (S.D.N.Y. 2018).

The parties do not dispute that Khandekar copied and viewed Predictors containing trade secrets. And as discussed, Khandekar breached the Employment Agreement and therefore used improper means to access those trade secrets. Unlike the DTSA, however, New York trade-secrets law does not create liability for mere acquisition. The question comes down, once again,

to whether Khandekar *used* KCG's trade secrets. And he did—for the same reasons as under the federal statute. Khandekar analyzed KCG's trade secrets to increase his personal knowledge and skillset, thereby using them.

The cases Khandekar cites to the contrary are all inapt, because they involve only acquisition and no use. For example, in *Lewin v. Richard Avedon Foundation*, the plaintiff alleged that the defendant misappropriated a trade secret by stealing a notebook “detailing how to create certain . . . prints,” access to which “could [have] provide[d] [the defendant] with the ability to reproduce impermissibly [plaintiff's] photography.” 2015 WL 3948824, \*30 (S.D.N.Y. 2015). The Court denied the New York trade-secrets claim because the plaintiff had not put forward any evidence that the defendant had actually taken photographs of the trade secrets in the notebook, shared those photographs, or utilized them in any way. *Id.* at n.25. As with the federal claim, this would be a different case if Khandekar had merely copied the files into his directory. But he did far more than copying—he reviewed them, organized them based on their utility, and extracted useful information from them to develop his expertise. Khandekar's claim about staleness fails for the same reason. He argues that because the trade secrets “are aged,” they “have likely grown stale” and thus they are less likely to be used. Def. Br. at 15. But he provides no facts to support this staleness theory. *See Ridinger*, 651 F.3d at 317 (“[C]onclusory statements, conjecture, and inadmissible evidence are insufficient to defeat summary judgment.”). And besides, even if the trade secrets are now stale, the undisputed record demonstrates that Khandekar used them when they were still ripe—and liability attached at that time. The Court thus concludes that KCG is also entitled to summary judgment on its state-law trade-secrets claim.

## VII. KHANDEKAR DID NOT VIOLATE THE COMPUTER FRAUD AND ABUSE ACT

KCG next argues that Khandekar violated the Computer Fraud and Abuse Act (CFAA), and both parties have cross-moved for summary judgment on this issue. Because there is no genuine dispute that Khandekar did not exceed his authorized access to KCG's systems, one of the statute's requirements for liability is not met, and Khandekar is entitled to summary judgment on this claim.

The CFAA was enacted in 1986 solely as a criminal statute, designed to address the “then-novel problem of [computer] hacking.” *Hancock v. Cty. of Rensselaer*, 882 F.3d 58, 63 (2d Cir. 2018). Ten years later, Congress added a limited civil cause of action. *Fischkoff v. Iovance Biotherapeutics, Inc.*, 339 F. Supp. 3d 408, 417-18 (S.D.N.Y. 2018). As relevant here, the statute provides a cause of action against “Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer.” 18 U.S.C. § 1030(a)(2)(C). The CFAA creates many requirements for civil liability. The Court focuses on one: whether Khandekar accessed KCG's computers “without authorization or exceed[ed] authorized access” in doing so. *Id.* The statute defines “exceeds authorized access” as follows: “The term ‘exceeds authorized access’ means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to so obtain or alter.” *Id.* § 1030(e)(6).

The meaning of this requirement has been heavily debated and divided the Courts of Appeals. In 2015, the Second Circuit formulated the standard that governs here. *See United States v. Valle*, 807 F.3d 508 (2d Cir. 2015). In *Valle*, a police officer searched a police database for an individual's personal information, acting with no law-enforcement purpose. The Court concluded that the officer did *not* exceed his authorized access to the Police Department's

database. This statutory requirement is met “only when [the defendant] obtains or alters information that he does not have authorization to access for any purpose which is located on a computer that he is otherwise authorized to access.” *Id.* at 511. Although *Valle* was a criminal case, the Supreme Court has instructed that courts analyzing statutes having “both criminal and noncriminal applications . . . must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context.” *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004); see *Fischkoff v. Iovance Biotherapeutics, Inc.*, 339 F. Supp. 3d 408, 418 (S.D.N.Y. 2018) (following the *Valle* standard in a civil case); cf. *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004) (noting that the rule of lenity applies in both contexts).

Courts have observed that “where an employee has certain access to a computer or system associated with her job, that access will be construed as unauthorized within the meaning of the CFAA only where it occurs after the employee is terminated or resigns.” *Poller v. BioScrip, Inc.*, 974 F. Supp. 2d 204, 233 (S.D.N.Y. 2013); accord *Amphenol Corp. v. Paul*, 993 F. Supp. 2d 100, 110 (D. Conn. 2014), *aff’d*, 591 Fed. Appx. 34 (2d Cir. 2015). For example, in *Apple Mortgage Corp. v. Barenblatt*, the defendants, after resigning, continued to receive emails on their cell phones because the plaintiff “had not changed the codes on its computer system in the days following the defendants’ resignation.” 162 F. Supp. 3d 270, 277 (S.D.N.Y. 2016). The Court denied the defendants’ motion for summary judgment on the CFAA claim because there was “evidence that after the employees resigned[,] they accessed emails from the [employer’s] system on their phones and read, forwarded, or deleted emails,” meaning that there was “a triable issue of fact as to whether they acted ‘without authorization’ when they accessed, deleted, or forwarded these emails.” *Id.* The Court in *BioScrip* succinctly explained this rule as follows: “No language in the CFAA supports the argument that authorization to use a computer ceases

when an employee resolves to use the computer contrary to the employer's interest, so long as that individual still *technically* possesses the right of computer access pursuant to his employ. In other words, exploitative or disloyal access to an employer's computer will not render otherwise permissible access unauthorized within the CFAA's meaning." *BioScrip, Inc.*, 974 F.Supp.2d at 232 (emphasis added); *see also Univ. Sports Pub. Co.*, 725 F.Supp.2d at 383 ("[A]n employee with authority to access his employer's computer system does not violate the CFAA by using his access privileges to misappropriate information.") (citing cases).

Khandekar thus argues that he did not "exceed authorized access" within the statute's meaning. Def. Br. 34-35. He is correct. The parties do not dispute that Khandekar had "technical access" to the files at issue. There were no access restrictions in place that he skirted. There was no decrypting to be done. He used his regular work login to access and copy the files at issue. To be sure, copying the files was against KCG policy. In that sense, it was unauthorized. But it was not unauthorized *access*, nor did it exceed Khandekar's authorized *access*, because Khandekar clearly had the ability to copy and view these files. KCG's claim under the Computer Fraud and Abuse Act thus fails as a matter of law, and Khandekar is entitled to summary judgment on this issue.

### **VIII. KCG IS ENTITLED TO A NARROW INJUNCTION**

To summarize, Khandekar has breached his Employment Agreement, violated the Defend Trade Secrets Act, and violated New York trade-secrets law. The Court has awarded KCG attorney's fees and expenses, including the cost of KCG's investigation into Khandekar's conduct. The remaining issues are whether KCG is entitled to injunctive relief and, if so, that relief's scope. The Court concludes that the appropriate relief is to prohibit Khandekar from using or disseminating the information he obtained from his unauthorized review of trade secrets while at KCG between November 2016 and May 2017.



### **A. The Requirements for Injunctive Relief Are Met**

“To obtain a permanent injunction, a plaintiff must succeed on the merits and show the absence of an adequate remedy at law and irreparable harm if the relief is not granted.” *Roach v. Morse*, 440 F.3d 53, 56 (2d Cir. 2006) (internal quotation marks and citation omitted). These requirements are met here.

To start, KCG has succeeded on the merits: the Court has awarded it summary judgment on its breach-of-contract claim, its DTSA claim, and its New York common-law claim. It has also shown that it will be irreparably harmed absent injunctive relief. The Second Circuit has explained that it is not appropriate to presume irreparable injury “[w]here a misappropriator seeks only to use [trade] secrets—without further impairment or irreparable impairment in value—in pursuit of profit.” *Faiveley Transp. Malmo AB v. Wabtec Corp.*, 559 F.3d 110, 118–19 (2d Cir. 2009). Applying this standard, courts have found a lack of irreparable harm where “defendants have no incentive to disseminate any trade secrets they may have misappropriated from plaintiffs, as defendants would want to use that information and maintain its confidentiality for their own pecuniary benefit.” *Golden Krust Patties, Inc. v. Bullock*, 957 F. Supp. 2d 186, 197 (E.D.N.Y. 2013). However, the Second Circuit has made clear that a “rebuttable presumption of irreparable harm might be warranted in cases where there is a danger that, unless enjoined, a misappropriator of trade secrets will disseminate those secrets to a wider audience or otherwise irreparably impair the value of those secrets.” *Faiveley*, 559 F.3d at 118–19. As one Court explained, “misappropriation of trade secrets by a competitor is not necessarily irreparable harm, because that entity is likely motivated to protect the secret to serve its own purposes, and . . . injunctive relief is inappropriate absent incentive to further disseminate or impair the value of the information.” *Genworth Fin. Wealth Mgmt., Inc. v. McMullan*, 721 F. Supp. 2d 122, 128–29 (D. Conn. 2010).

“Even where a trade secret has not yet been disclosed, irreparable harm may be found based upon a finding that trade secrets will inevitably be disclosed where, as here, ‘the movant competes directly with the prospective employer and the transient employee possesses highly confidential or technical knowledge concerning marketing strategies, or the like.’” *Estee Lauder Companies Inc. v. Batra*, 430 F.Supp.2d 158, 174 (S.D.N.Y. 2006) (quoting *EarthWeb, Inc. v. Schlack*, 71 F.Supp.2d 299, 309 (S.D.N.Y. 1999)). The presumption of irreparable harm afforded trade secrets is particularly appropriate when information at risk of disclosure is highly technical or can be used only by a few specialized businesses. *See, e.g., International Business Machines Corp. v. Johnson*, 629 F.Supp.2d 321, 335 (S.D.N.Y. 2009); *International Business Machines Corp. v. Papermaster*, 2008 WL 4974508, at \*8 (S.D.N.Y. 2008).

Here, KCG faces irreparable harm because Khandekar does not merely seek to use its trade secrets or keep them to himself. Instead, if Khandekar resumes producing Predictors for another financial-services firm, he could disseminate the trade secrets he improperly acquired to a wider audience—namely, members of his new firm. And this dissemination would also impair the value of KCG’s secrets. Predictors are valuable only because they are proprietary; if other firms can deduce the same market information from the same set of variables, KCG’s Predictors would lose their competitive edge. In short, if Khandekar is employed at a financial-services firm that develops Predictors, he could rely on the knowledge he gleaned from his improper acquisition and use to develop Predictors predicated on those trade secrets. *See Roach v. Morse*, 440 F.3d 53, 56 (2d Cir. 2006) (“the question is not whether the plaintiff has suffered irreparable harm, but whether it will be irreparably harmed in the absence of an injunction. In other words, the injunction must prevent or remedy the harm.”). The Court therefore finds that the irreparable-harm requirement is met.

Moreover, monetary relief alone would be insufficient to remedy this harm. The Second Circuit has explained that “an award of damages [may not] provide a complete remedy” if there is “a danger that, unless enjoined, a misappropriator of trade secrets will disseminate those secrets to a wider audience or otherwise irreparably impair the value of those secrets.” *Faiveley*, 559 F.3d at 118. That is the case here. As noted, if Khandekar uses the Predictors at one of KCG’s competitors, those secrets would be shared with other employees of that firm. And once again, this use would also impair the trade secrets’ value. Predictors are valuable to KCG because they allow the firm to execute trades that other players on the market are not. If other firms begin making the same trades, KCG’s Predictors will lose their competitive advantage and become less valuable. *See* Def. Ctr. ¶ 2. The requirements for injunctive relief are thus met.

**B. KCG’s Requested Injunction is Overbroad, and Narrower Relief is Appropriate**

The Second Circuit has explained that “[i]n all cases, the [injunctive] relief should be ‘narrowly tailored to fit specific legal violations’ and avoid ‘unnecessary burdens on lawful commercial activity.’” *Faiveley*, 559 F.3d at 119 (quoting *Waldman Pub. Corp. v. Landoll, Inc.*, 43 F.3d 775, 785 (2d Cir. 1994)). The DTSA provides a similar rule: “In a civil action brought under this subsection with respect to the misappropriation of a trade secret, a court may . . . grant an injunction . . . to prevent any actual or threatened misappropriation described in paragraph (1) on such terms as the court deems reasonable, provided the order does not— (I) prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows; or (II) otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business.” 18 U.S.C. § 1836(b)(3)(A). New York law, in turn, requires that restraints on competition like the proposed injunction here be “no greater

than is required for the protection of the legitimate interest of the employer,” not impose an undue hardship on the employee, and not be injurious to the public. *BDO Seidman v. Hirschberg*, 93 N.Y.2D 382, 388-89 (N.Y. 1999).

The parties dispute the scope of injunctive relief here. KCG seeks to enjoin Khandekar from developing Predictors “for his own use or use by any competitors of KCG for market-making.” Pl. Reply Br. at 23. Khandekar argues that this restriction is overbroad, as “it would enjoin him from developing any kind of Predictor, as opposed to a narrower restriction tailored to Predictors of the same types as those he worked on or improperly viewed.” *Id.* Khandekar claims that KCG’s requested relief would ban him—for life—from working in his desired career. Pl. Ctr. ¶ 31. KCG minimizes the scope of its requested relief, claiming that the “injunction only restricts Khandekar from performing one very specific task in a very specific business area—*i.e.*, developing Predictors for use in market making activities.” Pl. Ctr. ¶ 31. To the contrary, says KCG, Khandekar is well-qualified for other types of employment in the financial-services industry, in which he could utilize his skills like quantitative methods and statistical analysis. *Id.* ¶¶ 31, 32.

The Court agrees that KCG’s requested relief is overbroad. It would prohibit Khandekar from working on Predictors in any capacity, in perpetuity. Yet the parties agree that this was Khandekar’s primary role at KCG, and would have been his role at Two Sigma. Such an injunction would foreclose him from this chosen career path. KCG is correct that he could seek other types of employment in the same industry, but that misstates the level of generality of this inquiry. For example, prohibiting a trial attorney from practicing litigation is no less intrusive because she could in theory also practice transactional law. The same is true here, and KCG’s requested relief would thus impose substantial hardship on Khandekar. KCG bears the burden to

show why this restriction is needed, as opposed to the narrower restriction of prohibiting Khandekar from using the knowledge he improperly gained from other Quants' Predictors.

KCG provides two reasons why the Court should enjoin Khandekar from developing *any* Predictors, as opposed to this narrower restriction. First, it claims that "Khandekar has demonstrated his willingness to misappropriate KCG's information; therefore, he cannot be trusted to develop only new Predictors that are entirely unrelated to the ones he improperly acquired from KCG." Second, it argues that the injunction "cannot be restricted by Predictor type because KCG would no way of monitoring Khandekar's compliance with such a restriction." *Id.* Neither argument is persuasive. To start, previous misappropriation by a defendant—and his "untrustworthiness" as a result—cannot justify the breadth of an injunction. In any case in which the Court is considering injunctive relief, the plaintiff will have prevailed on the merits and have shown misappropriation. KCG bears the burden to show why the *specific* relief it requests is appropriately tailored and does not impose an undue hardship, and this argument fails to move the ball. KCG's compliance argument is similarly without merit. It has introduced no facts into the record proving this monitoring problem. It also provides no authority for the proposition that a purported inability to monitor compliance by itself justifies such overbreadth. And this is a slippery slope—many trade-secret cases involve industries with potential monitoring difficulties, yet every injunction in such cases cannot be industry-wide. The narrower injunction is all that is warranted to "to prevent any actual or threatened misappropriation" of KCG's trade secrets. 18 U.S.C. § 1836(b)(3)(A). The Court thus concludes that the appropriate relief is to prohibit Khandekar from using or disseminating the information he obtained from his unauthorized review of trade secrets while at KCG.

## IX. CONCLUSION

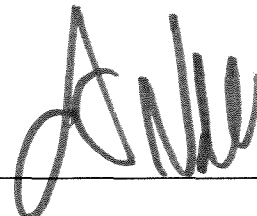
The Court grants and denies summary judgment in part to each party. KCG is entitled to summary judgment on its breach-of-contract, DTSA, and New York common-law claim. KCG is also entitled to summary judgment on Khandekar's breach-of-contract and bad-faith counterclaims. Khandekar is entitled to summary judgment on KCG's CFAA claim. This resolves Dkt. Nos. 114 and 129.

Khandekar is ORDERED to pay KCG's attorney's fees, costs, and expenses, including its investigation costs. Khandekar is further ENJOINED from using or disseminating, in any way, the trade secrets he reviewed without authorization at KCG between November 2016 and May 2017.

SO ORDERED.

Dated: March 12, 2020

New York, New York

A handwritten signature in dark ink, appearing to read 'Alison J. Nathan', is written over a horizontal line.

ALISON J. NATHAN

United States District Judge